Patent
Attorney's Docket No. 1032326-000161

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AMENDMENT**
Jean-Sebastien Coron et al.	Group Art Unit: 2131
Application No.: 09/913,884	Examiner: Matthew T Henning
Filed: March 8, 2002	Confirmation No.: 5848
For: METHOD FOR COUNTERMEASURE IN AN ELECTRONIC COMPONENT USING A SECRET KEY ALGORITHM	

RESPONSE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated February 8, 2007, Applicants respectfully request reconsideration and withdrawal of the rejection of the claims.

Claims 24-37 were rejected under 35 U.S.C. § 103 on the basis of U.S. Patent No. 6,278,783 (identified as "Kocher1") in view of U.S. Patent No. 6,327,661 (identified as "Kocher2"). It is respectfully submitted that, even if the teachings of the Kocher2 patent are applied to the system of the Kocher1 patent, the result would not be the same as the subject matter of the rejected claims.

In rejecting the claims, the Office Action states that the Kocher1 patent discloses the operations that are performed in the conventional DES algorithm, and goes on to acknowledge that it does not disclose the claimed steps of selecting a first random value having the same size as the data being permuted, performing an exclusive-OR operation between the data being permuted and the first random value to generate a second random value, executing the permutation operation on each of

the first and second random values, to generate respective first and second random results, and performing an exclusive-OR operation between the first and second random results to produce a final permuted result. To this end, therefore, the Office Action relies upon the Kocher2 patent as disclosing such subject matter, with particular reference to column 10, line 50 to column 13, line 19. It is respectfully submitted that the Kocher 2 patent does not disclose these claimed features.

Claim 24 recites that a first random value is selected, a second random value is generated from this first random value, and the permutation operation is executed "on each of the first and second random values, to generate respective first and second random results". Thus, the claim recites that two permutation operations are performed, respectively on the first and second random values. The claim further recites that an exclusive-OR operation is performed on the results of these two permutation operations. These concepts are depicted, for example, in Figure 3 of the present application.

It is respectfully submitted that the cited passage in the Kocher2 patent does not disclose these operations. As best as can be understood, column 12, lines 56-60 of the Kocher2 patent discloses that a single permutation operation is performed. Applicants are unable to identify where the patent discloses that two random values are obtained, a permutation operation is executed on each of the two random values, and the results of these two permutation operations are combined through an exclusive-OR operation. Consequently, any possible combination of the Kocher1 and Kocher2 patents would not lead a person of ordinary skill in the art to the claimed subject matter.

If the rejection of the claims is not withdrawn, the examiner is requested to identify, with particularity, (1) what are being interpreted to be the first and second random values in the Kocher2 patent, (2) where the Kocher2 patent discloses that a permutation operation is performed on each of these two random values, and (3) where the patent discloses that an exclusive-OR operation is performed on the results of such permutation operations. In the absence of such showings, it is respectfully submitted that proper support has not been established for the rejection of the claims. Specifically, the Office Action has not shown that every limitation recited in the claims is disclosed in the prior art, as required for a prima facie case of obviousness. MPEP § 2143.03

Reconsideration and withdrawal of the rejections, and allowance of pending claims 23-37 is respectfully requested.

Respectfully submitted,
BUCHANAN INGERSOLL & ROONEY PC

Date: May 8, 2007

By: /james labarre/

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620